Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

- **Contraseñas fuertes que puedas recordar**
- **Jamás compartas tus contraseñas**
- **Utiliza tus contraseñas de manera segura**

Protege tus contraseñas

EDITOR INVITADO

Eric Cole es el editor invitado para el boletín OUCH! de mayo. El Dr. Cole es el fundador de “Secure Anchor Consulting”, ha sido director de tecnología de grandes organizaciones y es miembro distinguido del Instituto SANS. Apasionado en ayudar a las organizaciones a hacer lo correcto para mejorar su seguridad. Puedes encontrar más información sobre su trabajo en http://www.securityhaven.com

RESUMEN

Las contraseñas son las llaves de entrada a tu reino, combinadas con tu nombre de usuario son el medio más común para identificarte y acceder a tu computadora, sitios web o información. Desafortunadamente, con mucha frecuencia las personas hacen poco por proteger sus contraseñas, usando combinaciones sencillas como “123456”, “password”, “qwerty” o “abc123”. En algunos casos, la gente simplemente utiliza el nombre de su mascota o su fecha de nacimiento, información que fácilmente puede encontrarse en Internet, por ejemplo en Facebook. Si un atacante obtuviera tu contraseña, podría robar tu identidad digital, acceder a tus cuentas bancarias o incluso ingresar a la información confidencial de tu organización, provocando un desastre. También es importante recordar que si alguien roba tu contraseña, ¡podrían acusarte por lo que hagan con tu cuenta! Para proteger mejor a tu familia, a tu organización y a ti mismo, aprenderemos en qué consiste hacer una buena contraseña y cómo utilizarla de manera segura.

CONTRASEÑAS FUERTES

Los criminales cibernéticos han desarrollado programas automáticos capaces de adivinar o romper por la fuerza tus contraseñas. Para protegerte de esto, es importante que tus contraseñas sean difíciles de adivinar y fáciles de recordar. Algunas recomendaciones son:

- Tu contraseña debe contar con al menos un número.
- Tu contraseña debe tener al menos una letra MAYÚSCULA.
- Tu contraseña debe contar al menos con un símbolo.
- Recomendamos que tu contraseña tenga como mínimo 12 caracteres de longitud. Cuando se trate de sitios o información confidencial, recomendamos una longitud de 15 caracteres. Consulta con los encargados de tu organización sobre las políticas de contraseñas.

A primera vista puede parecerte complicado. Sin embargo,

Protege tus contraseñas

usando la primera letra de cada palabra en un enunciado, obtenemos una contraseña más fácil de recordar. Por ejemplo, el siguiente enunciado es muy sencillo de recordar:

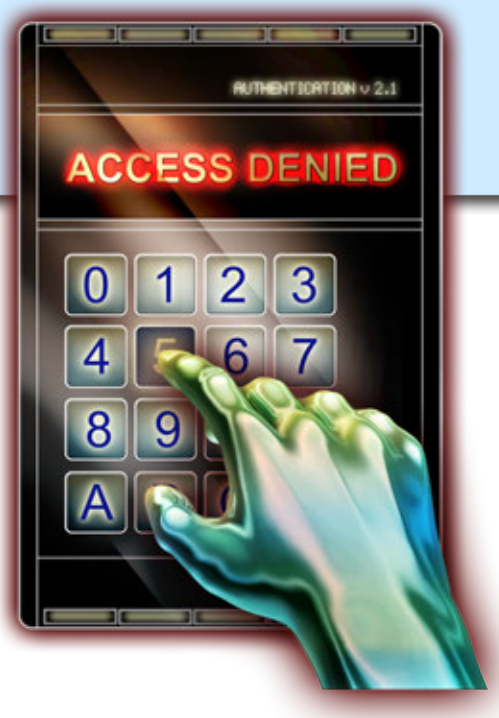
Mi 2do hijo nació en el Hospital Centro Médico a las 6:30pm

Podemos usar este enunciado para crear una contraseña como la siguiente:

M2hn@HCM@6:30pm

Lo que hicimos, fue simplemente usar la primera letra de cada palabra. Algunas de estas letras se escribieron en mayúscula. Además, sustituimos las preposiciones por el símbolo "@". Finalmente, incluimos la hora. Esta es una contraseña larga y compleja, difícil de adivinar pero fácil de recordar.

La clave para proteger tus contraseñas es utilizar contraseñas fuertes difíciles de adivinar, nunca las compartas y sé cuidadoso cuando las utilices.



PROTEGE TUS CONTRASEÑAS

Ten en cuenta que no es suficiente establecer contraseñas fuertes. No importa si tienes la contraseña más compleja del mundo, de no considerar los siguientes pasos, al final tus contraseñas serían comprometidas.

1. ¡No seas una víctima más! Una de las formas más comunes que los criminales cibernéticos utilizan para robar tus contraseñas es infectar tu computadora. Una vez comprometida, estos intrusos instalan malware especializado que captura todo lo que escribes con el teclado, incluyendo nombre de usuario y contraseña para banca en línea. Cuando accedes a tu banco, tu información es robada automáticamente y reenviada al criminal cibernético. Entonces, estos sujetos pueden tener acceso a tu cuenta bancaria, hacerse pasar por ti y literalmente robar todo tu dinero. Para defenderte, asegúrate que la protección de tu computadora sea la adecuada, que incluya la función de actualizaciones automáticas y cuente con la última versión del antivirus.

2. Asegúrate de usar distintas contraseñas para distintas cuentas. Por ejemplo, nunca utilices las contraseñas de cuentas personales, como Facebook, YouTube o Twitter en tus cuentas de trabajo o bancarias.

Protege tus contraseñas

De esta forma, si una de tus contraseñas es robada, las demás estarán a salvo.

3. Nunca compartas tu contraseña con nadie, así sea tu jefe o alguien de soporte técnico. Recuerda, tu contraseña es un secreto, si alguien más lo sabe, tu contraseña ya no es segura.

4. Nunca utilices una computadora pública, como las que están en hoteles o bibliotecas para ingresar a tu cuenta. Cualquiera persona puede hacer uso de estas computadoras e infectarlas con códigos maliciosos para que capturen todo lo que escribas. Sólo ingresa a tus cuentas de trabajo o personales desde equipos confiables bajo tu control.

5. En algunas ocasiones, tienes que emplear tantas contraseñas que no puedes memorizar todas, y almacenarlas puede ser tu única opción. Si las escribes, asegúrate de guardarlas en un lugar seguro al que sólo tú tengas acceso y nunca las dejes a la vista de los demás. Otra opción es almacenar tus contraseñas empleando aplicaciones de cifrado, diseñadas especialmente para hacerlo, tanto en smartphones como en computadoras. Puedes encontrar ejemplos de estas herramientas en: http://tinyurl.com/622v9m2 y http://tinyurl.com/2p385o

6. Sé cuidadoso con los sitios web que te pidan configurar preguntas personales. Estas preguntas suelen utilizarse por si olvidas la contraseña de tu cuenta o necesitas restablecerla. El problema con estas preguntas es que las repuestas pueden encontrarse en Internet, como en tu página personal de Facebook. Asegúrate de que tus respuestas personales no tengan información que esté publicada en Internet. Si el sitio web ofrece otras opciones de restauración como mensajes SMS a tu smartphone, considéralas.

7. Si crees que tu contraseña ha sido comprometida o tienes razones para creer que ya no es secreta, contacta al personal de soporte y cambia tu contraseña inmediatamente desde una computadora confiable bajo tu control.

APRENDE MÁS

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti. Visítanos en http://www.securingthehuman.org.

VERSIÓN EN ESPAÑOL

UNAM-CERT, único equipo de respuesta a incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país. Sitio web http://www.seguridad.unam.mx, síguelo en Twitter @unamcert.

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy
Versión en español a cargo de UNAM-CERT: Cecilia Espinosa, Israel Andrade, Galvy Cruz, Mauricio Andrade, Rubén Aquino